

Notes on Computer Networks

What is the big deal about computer networks?

- **Allows two or more computers to communicate**
- **Benefits**
 - Programs can be shared - software packages can be installed onto the file server and accessed by all individual workstations at the same time. This reduces cost, maintenance and makes upgrades easier.
 - You can access your work from any workstation on the network. Very handy if you have to change computer every time you go to a different classroom.
 - Data can be shared by all users at the same time. Many people can access or update the information held on a database at the same time. Thus information is up to date and accurate.
 - Users can communicate with others on the network by sending messages and sharing files.
 - Individual workstations do not need a printer; one high quality printer can now be shared by everyone, thus cutting costs.
 - Networks provide security. A user must have the correct Password and User ID in order to be able to access the information on the network.
 - Private areas on the network can be set up that allows each user to store their personal files. The only other person who can access these files is the 'system administrator' who looks after the network.
- **Disadvantages**
 - Networks can be expensive to set up. They often involve taking up floors and ceilings to lay hundreds of feet of cables
 - The File Server needs to be a powerful computer, which often means that it is expensive.
 - Networks are vulnerable to security problems. Hackers, disgruntled employees or even competitors might try to break into the system to read or damage crucial information. Much effort is spent preventing unauthorized access to data and software.
 - If the main File Server breaks down, then the whole system becomes useless and no-one can carry on working.
 - Because networks are often complicated, they need expensive expert staff to look after them.
 - As the number of users increase on the network, the performance of the system can be affected and things start to slow down.
 - Malware, such as worms, easily spread on computer networks and not on stand alone computers.
- **Main types of networks**
 - **LAN** – Local Area Network
 - A computer network in the same geographical location
 - Many small LAN's can make up a larger LAN, as long as they are all within the same geographical location (computer labs in different classrooms that are all in the same building)
 - Uses Ethernet cable or wireless (radio waves) to send data between networked computers

- **WAN – Wide Area Network**
 - A computer network that crosses geographical boundaries
 - Many small WAN's can make up a larger WAN
 - The Internet is the biggest WAN as it is comprised of all of the smaller WAN's and LAN's in the world connected to the Internet
 - Uses Fiber Optic Cable, Satellite technology, existing TV cable phone lines to send data over the network

- **Ethernet cable**
 - Used in LAN's
 - Limits on it's length (when an Ethernet cable is longer than 328 feet, data transmitted over the cable is dropped)

- **Routers**
 - Needed to create a computer network
 - Can assign individual computers and network printers on a computer network individual IP addresses to create a sub-network
 - Directs data across the network

- **Wireless Networks**
 - Based on the 802.11 standard
 - Benefits
 - Cheaper to set up because you don't have to buy and install network cable
 - Allows mobility with laptops, PDA's smart phones, and PSP's
 - Disadvantages
 - Harder to secure, potential for unauthorized persons within range of the wireless signal access to your network and personal data
 - Wireless Router
 - receives the radio signal and decodes it - it sends the information to the Internet using a physical, wired Ethernet connection
 - most home routers are a combination of wired and wireless
 - Types of security
 - Wired Equivalency Privacy (**WEP**) - WEP encrypts data transmitted over the WLAN
 - A 64-bit WEP encryption is almost always entered by users as a string of 10 Hexadecimal (Hex) characters (0-9 and A-F)
 - A 128-bit WEP encryption is almost always entered by users as a string of 26 Hexadecimal (Hex) characters (0-9 and A-F)
 - 128 bit encryption is more secure because it takes longer to break the passcode because of its increased number of characters.
 - WiFi Protected Access (**WPA**) - WPA-PSK is an extra-strong encryption where encryption keys are automatically changed (called **rekeying**) and authenticated between devices after a specified period of time, or after a specified number of packets has been transmitted. This is called the **rekey interval**. WPA-PSK is far superior to WEP and provides stronger protection for the home/SOHO user for two reasons. The process used to generate the encryption key is very rigorous and the rekeying (or key changing) is done very quickly. This stops even the most determined hacker from gathering enough data to break the encryption.

- Media Access Control (**MAC**) address filtering - a hardware address that uniquely identifies each node of a network you can identify which nodes have permission to access a network by their individual MAC address.
- **Network types:**
 - **Internet** - The Internet was created back in 1969, during the Cold War, by the United States military. It was meant to be a "nuke-proof" communications network. Today, the Internet spreads across the globe and consists of countless networks and computers, allowing millions of people to share information. Data that travels long distances on the Internet is transferred on huge lines known collectively as the Internet backbone. The Internet is now maintained by the major Internet service providers such as MCI Worldcom, Sprint, GTE, ANS, and UUNET. Because these providers make huge amounts of revenue off the Internet, they are motivated to maintain consistent and fast connections which benefits everyday Internet users like you and me.

The Internet and the World Wide Web are not the same thing. The World Wide Web is the Internet feature that allows you to visit web pages from all over the world. It is one of the many features of the Internet. E-mail, FTP, and Instant Messaging are also features of the Internet.

- **Intranet** - Intranet is an internal or private network using Internet technology that can only be accessed within the confines of a company, university, or organization
- **Extranet** - An extranet is a private network that uses Internet technology and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company. (When you log onto MySpace, you enter an Extranet.)
- **VPN (Virtual Private Network)** - A VPN refers to a network that is connected to the Internet, but uses encryption to scramble all the data sent through the Internet so the entire network is "virtually" private.
- **Network Security Issues:**
 - Who has access to the network?
 - Is access controlled by physical barriers?
 - network is in a locked room or building
 - Is access controlled by appropriate authentication procedures
 - What type of authentication is used to access the network?
 - Password/username (are users required to regularly change their passwords)
 - Biometrics
 - Security questions
 - RFID tags
 - Bar codes
 - CAPTCHA systems
 - When used in a company, are company policies in place to identify who has access to the network?
 - When used in a company, are user permissions clearly established within the server software or does everyone have permission to the same level of network folders and files?
 - Is network users' network activity monitored?
 - Is anti-virus and anti-spyware software installed on all client computers and is it kept up-to-date?

- Is a Firewall used and is it configured appropriately for the network it protects?
- Is there a network policy that specifically outlines what is and what is not allowed to be done on the network by the network users?
- **Social - ethical concerns:**
 - **Is the Internet a positive or a negative development for our world?**
 - **Positives:**
 - Ability to communicate via teleconferencing or videoconferencing from any where in the world
 - Can do business with anyone from anywhere
 - Can shop from anywhere in the world
 - Skype is a free videoconferencing program and service
 - Marketing is easier, more wide-spread and less expensive for everyone
 - Anyone can open a business and advertise inexpensively with a website or participation in an auction site
 - Allows people to communicate with others from different countries and cultures, potential to create a more diverse populace
 - Chat rooms, forums, social networking sites, etc...
 - Sharing of files quickly from anywhere in the world
 - View events as they are happening from anywhere with “real-time”
 - Allows “virtual” educational opportunities for anyone with Internet access
 - On-line classes
 - Educational websites
 - Educational pod casts made available
 - On-line tutorials
 - **Negatives:**
 - Personal and financial information easily available to hackers because of form entries and online shopping
 - Viruses can easily travel through the Internet to steal personal and financial information from individual computers. This could result in financial ruin or identity theft.
 - People can pretend to be anyone of any age, race or gender to dupe unsuspecting computer users
 - MySpace and other social networking sites that allow members to post personal information and make it available to anyone, if they choose. Predator issues.
 - Scam artists making false claims of financial wealth to trick others out of their money
 - Easy to share files (music, photographs, movies, drawings, etc...) without regard to copyright laws
 - File to file peer sharing (Kazza, Limewire, Bearshare)
 - Information of **ALL** types is available to anyone surfing the Internet, whether appropriate or not.
 - Software designed to block inappropriate sites are not perfect. They can only block sites by IP Address, keywords or domain name. A deceptive web designer can publish an inappropriate website using appropriate text and file names and not be detected by a blocking program until it is discovered and manually blocked by the user by IP Address or domain name.

- Many “good” sites get blocked because blocking programs can not decipher between a truly good site verses an inappropriate site.
- Easy way to communicate and spread false and misleading information about someone or something.
- Real concerns about **Cyber Warfare** completely disabling major economies.
 - A "**cyber cold war**" is causing an eminent threat for the world's computers. Internet security company, McAfee, in their 2007 annual report stated that approximately 120 countries have been developing ways to use the Internet as a weapon and the targets are financial markets, government computer systems and utilities.
 - There are several methods of attack in cyber-warfare; this list is ranked in order of mildest to most severe.
 - **Web vandalism:** Attacks that deface web pages, or denial-of-service attacks. This is normally swiftly combated and of little harm.
 - **Propaganda:** Political messages can be spread through or to anyone with access to the internet.
 - **Gathering data.** Classified information that is not handled securely can be intercepted and even modified, making espionage possible from the other side of the world. See Titan Rain and Moonlight Maze.
 - **Distributed Denial-of-Service Attacks:** Large numbers of computers in one country launch a Denial of Service, an attempt to make a computer resource unavailable to its intended users, attack against systems in another country.
 - **Equipment disruption:** Military activities that use computers and satellites for co-ordination are at risk from this type of attack. Orders and communications can be intercepted or replaced, putting soldiers at risk.
 - **Attacking critical infrastructure:** Power, water, fuel, communications, commercial and transportation are all vulnerable to a cyber attack.